CENTRO DE CIBERSEGURIDAD INDUSTRIAL

EDICIÓN 2021

EL RINCÓN DEL COMPLIANCE EN LA INDUSTRIA

AUTOR

Juan Miguel Pulpillo

CDPSE (Certificado Ingeniero en Soluciones de Protección de Datos) por ISACA Internacional I Abogado Auditor en Entornos Tecnológicos del Registro AAULETEC del Icab I Certificado Auditor en Buen Gobierno, Gestión de Riesgos y Cumplimiento Normativo de Tüv Nord I Certificado Instructor de la Directiva (UE) 2019/1937, relativa a la protección de personas que informen sobre infracciones del Derecho de la Unión, y de Compliance. ASPERTIC (Barcelona-Bruselas) y Máster en Derecho de las Telecomunicaciones y Tecnologías de la Información por Universidad Carlos III de Madrid.

Experto Legal y Cumplimiento y Credencial Profesional Nivel Negro de Ciberseguridad Industrial del Centro de Ciberseguridad Industrial. CCI I Coordinador Andalucía I España del Centro de Ciberseguridad industrial, CCI I DPO del CCI.

Profesor y Miembro del Claustro del Máster en Derecho de las Telecomunicaciones y Tecnologías de la Información y Comunicación. Universidad Carlos III de Madrid

Profesor Claustro profesores del Título de Especialista Universitario en Diseño, gestión y dirección de proyectos de e-learning y b-learning; y del Título de Experto Profesional en Diseño y gestión de programas formativos en modalidad e-learning y b-learning de la UNED

Desde el año 2001 se dedica profesionalmente a analista de ciber inteligencia y ciberseguridad, compliance tecnológico y legal y GRC en tecnologías de la información y la operación.

CONTENIDO

ABSTRACTO

La evolución de las tecnologías digitales y de automatización que han permitido la digitalización industrial ha dado lugar a un nuevo conjunto de desafíos. Diferentes actores están recopilando ahora un gran volumen de información y otros activos intangibles, son propietarios y operadores, integradores, fabricantes y proveedores. Estos activos intangibles e información deben documentarse y asegurarse de acuerdo con las normas y regulación vigentes en cuanto al Cumplimiento y al Buen Gobierno. Unas normas y regulaciones cada vez más exigentes con requisitos de cumplimiento y accountability, o responsabilidad proactiva. Además, el aumento del uso de la información electrónica, las aplicaciones basadas en la nube, los dispositivos habilitados para IoT y el telecontrol industrial ha dado lugar a complejas operaciones de prestación de control y automatización industrial que son objetivos principales para los ciberataques. Dados los atributos de información, de los activos intangibles y, en su caso, su carácter de infraestructura crítica, estos ciberataques son más comúnmente dirigidos en la industria, que incluyen activos de información, no personal y personal, que suele caracterizarse por su ubicuidad; activos tecnológicos; activos de personas; activos comerciales; activos organizativos; y el impacto de tales ataques también se siente más severamente

En el primer artículo se analiza una nueva estrategia de gestión de riesgos de ciberseguridad industrial formalizada y evidenciada, basada en una sólida gestión de identidades, en una identificación y gestión activos intangibles e información y siguiendo un enfoque de cumplimiento cibernético, puede ayudar a las organizaciones industriales a proteger sus operaciones y su red IT y OT contra estas amenazas en evolución y muchos incumplimientos.

Al igual que para ganar un pleito, tan importante es tener razón, como saber probar que se tiene derecho a aquello que se solicita, en el Compliance es imprescindible implantar el Sistema de Compliance y tener la capacidad de probarlo. Lo que pone de manifiesto la relevancia práctica, por un lado, de gestionar de una manera adecuada la documentación y archivos del Sistema, y por otro lado, de la actividad probatoria y la necesidad de conocer debidamente los aspectos más destacados de la misma. En el segundo artículo, se analiza la actividad probatoria proactiva, o generación de evidencias tecnológicas o digitales, del Sistema de Compliance Industrial, a través del análisis forense informático. Utilizamos el análisis forense informático como herramienta para generar pruebas de Cumplimiento desde el diseño.

REDEFINIR LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD INDUSTRIAL DESDE EL CUMPLIMIENTO Y EL BUEN GOBIERNO

Con un aumento exponencial en el número de dispositivos conectados, la descentralización de la fuerza de trabajo y las aplicaciones y sistemas habilitados para la nube, los perímetros de seguridad previamente bien definidos se han desenfocado. Los CIO, los CEO y los CISO, junto con la incorporación de un nuevo puesto de Chief Government and Compliance (CGC), ahora deben proteger toda la industria en los procesos de digitalización, atender los requerimientos y obligaciones existentes en cuanto a la regulación y normativa y, al mismo tiempo, permitir a ciertos actores acceder a los sistemas de control y automatización industrial y a otros activos desde cualquier lugar, utilizando múltiples canales y dispositivos. Sin embargo, estos avances en cuanto a la digitalización industrial y su ciberseguridad, vienen con un conjunto único de desafíos en cuanto a las obligaciones de Cumplimiento y Buen Gobierno.

El CGC puede evaluar los procesos ejecutivos de toma de decisiones en busca de evidencia de que estos temas están recibiendo suficiente atención, para dar su opinión sobre si este riesgo se está gestionando en el nivel estratégico más fundamental.

El sector industrial en cuanto a su digitalización comprende diferentes tipos de actores con diferentes exigencias de requisitos y obligaciones en cuanto a los activos intangibles y a la ciberseguridad dependiendo del entorno, la ubicación, la entidad y el rol. Los usuarios empresariales, de TI, de OT y otros usuarios de operaciones y mantenimiento, así como los integradores, fabricantes y proveedores, requieren accesos a diferentes aplicaciones, información y otros activos intangibles. Sin embargo, en el sector industrial, en un proyecto de digitalización industrial, los actores internos y los externos, en modo presencial o en remoto, son la mayor amenaza para una organización. La complejidad de los flujos de trabajo y activos en este ecosistema altamente regulado presenta otro desafío. Rodeados de una necesidad cambiante de requisitos y obligaciones que hacen que la infraestructura de seguridad y cumplimiento sea altamente vulnerable y la pérdida de eficacia y eficiencia de la organización una posibilidad.

De esta manera, se identifican vulnerabilidades, con efectos en el cumplimiento, que pueden resultar de deficiencias en el diseño, integración y /o mantenimiento de los sistemas, así como fallas en diversos aspectos de ciberseguridad. En general, cuando se exponen o explotan vulnerabilidades en la tecnología operativa y /o de la información, ya sea directamente (por ejemplo, contraseñas débiles que conducen a un acceso no autorizado) o indirectamente (por ejemplo, la ausencia de segregación de la red), puede haber implicaciones para la seguridad y la confidencialidad e integridad. y disponibilidad de información. Por lo que hay implicaciones para el cumplimiento. Además, cuando las vulnerabilidades operativas y / o de la tecnología de la información están expuestas o explotadas, puede haber implicaciones para la seguridad, particularmente cuando los sistemas críticos (por ejemplo, la navegación de puentes o los sistemas principales de propulsión) están comprometidos. Por lo que hay implicaciones para el cumplimiento.

La gestión eficaz del riesgo de ciberseguridad también debe considerar los impactos de seguridad y protección que resultan de la exposición o explotación de vulnerabilidades en los sistemas de tecnología de la información y sobre los Activos Intangibles. Esto podría ser el resultado de una conexión inapropiada a los sistemas de tecnología operativa o de lapsos de procedimiento por parte del personal operativo o de terceros, que pueden comprometer estos sistemas o Activos intangibles (por ejemplo, el uso inadecuado de medios extraíbles como un lápiz de memoria). Por lo que hay implicaciones para el cumplimiento.

En esta realidad flexible, interconectada y basada en la nube, la gestión de identidades, la gestión de activos intangibles y del cumplimiento, y la gestión de ciberseguridad tienen la clave para prevenir ciberataques, incumplimientos y de mantener o aumentar el valor de la organización frente a la competencia.

Estas tecnologías y amenazas que cambian rápidamente hacen que sea difícil abordar estos riesgos y las obligaciones legales solo a través de estándares técnicos. Por ello, será imprescindible adoptar Directrices con un enfoque de gestión de riesgos para los riesgos de ciberseguridad y de cumplimiento que sea resistente y evolucione como una extensión natural de las prácticas de gestión de seguridad y protección existentes.

MARCO DE LA DIGITALIZACIÓN INDUSTRIAL DESDE LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD INDUSTRIAL DESDE EL CUMPLIMIENTO YEL BUEN GOBIERNO

Cualquier organización industrial debe comenzar con el ciclo de vida de digitalización y gestión de activos intangibles y, a continuación, puede escalar verticalmente hasta el cumplimiento de la gobernanza y la auditoría.

Planificación y diseño

Los Documentos y Estudios Previos de esta etapa permitirán analizar las distintas alternativas posibles para la ejecución del proyecto desde los puntos de vista técnico-económico-cumplimiento y financiero, para poder tomar decisiones en relación con la realización o no del proyecto.

Esta capa ayuda a detectar, identificar, documentar, para proteger los activos intangibles implicados en el proyecto de digitalización o resultantes de la misma, identificar los derechos necesarios sobre los mismos de los sujetos participantes (propietario y operadores, integradores, fabricantes y proveedores), mapa de riesgos del el marco regulatorio y normativo del contexto externo e interno del proyecto desde su diseño, así como la evaluación de riesgos correspondientes y necesarios. De todo ello habrá que guardar evidencias de todo ello y de la supervisión realizada por parte del CGC.

Por ello, se han de identificar unos elementos funcionales que respalden la gestión eficaz del riesgo cibernético y de cumplimiento. Estos elementos funcionales no son secuenciales; todos deben ser simultáneos y continuos en la práctica y deben incorporarse de manera apropiada en un marco de gestión de riesgos:

- **Identificar:** definir las funciones y responsabilidades del personal para la gestión del riesgo de cumplimiento cibernético e identificar los sistemas, activos, datos y capacidades que, cuando se interrumpen, plantean riesgos, entre ellos riesgos de cumplimiento, para las operaciones de la industria.

- **Proteger:** Implementar procesos y medidas de control de riesgos, que incluye los riesgos de cumplimiento cibernético, y planificación de contingencias para proteger contra un evento cibernético-cumplimiento y garantizar la continuidad de las operaciones.

- **Detectar:** Desarrollar e implementar las actividades necesarias para detectar un evento cibernético y cumplimiento cibernético de manera oportuna.

- **Responder:** Desarrollar e implementar actividades y planes para proporcionar resiliencia y restaurar los sistemas necesarios para las operaciones o los servicios dañados debido a un evento cibernético, limitando o eliminando las consecuencias de incumplimientos.

- **Recuperar:** Identificar medidas para respaldar y restaurar los sistemas cibernéticos necesarios para las operaciones de envío afectadas por un evento cibernético, limitando o eliminando las consecuencias de incumplimientos.

Por otra parte, el proyecto de digitalización industrial, en esta fase, también se centrará en:

- La realización de los estudios de viabilidad de la digitalización necesarios.

- Ingeniería. Con un alto impacto en los Activos Intangibles a nivel de componentes, sistemas, personas, información y organización.

- Ciberseguridad desde el diseño, estableciendo una estructura para la gestión de riesgos atendiendo al análisis y evaluación de riesgos.

Aprovisionamiento

Esta capa ayuda a optimizar la gestión de compras de la industria, en base a las nuevas oportunidades que brinda la digitalización, como el acceso a un gran volumen de datos, control de gasto, gestión organizativa o el control de la cadena de suministro, que favorece nuevos conocimientos estratégicos sobre proveedores y sus mercados. Cuestión que fortalece la gestión de riesgos de proveedores y el cumplimiento. Por otra parte, el proyecto de digitalización industrial, en esta fase, también se centrará en:

Derechos y licencias sobre AI

Es imprescindible Identificar, documentar, evaluar los riesgos y planificar la explotación de los Activos Intangibles utilizados y resultantes de dicho proyecto de digitalización industrial.

Gestión de compras

La selección correcta de un proveedor añade un gran valor a la ventaja competitiva, pero tiene amplias implicaciones en cuanto al cumplimiento en muy diversos aspectos (medioambientales, blanqueo, penal, contractual, ciberseguridad, etc).

En las circunstancias actuales, los reguladores han reconocido que las empresas pueden necesitar volver a priorizar o retrasar razonablemente algunas actividades, como las revisiones continuas de diligencia debida de los clientes y proveedores, pero que no deben ajustar su apetito por el riesgo o suspender las actividades de monitoreo de transacciones. Cualquier reducción o demora en la actividad de seguimiento de la diligencia debida debe basarse adecuadamente en el riesgo, con atención centrada en las transacciones y los clientes - proveedores de mayor riesgo.

Por esto, a medida que la organización se enfrenta a las presiones de un posible entorno recesivo en 2021, los desafíos económicos pueden haber desviado la atención de la industria de los riesgos de cumplimiento, ya que busca ser lo más competitiva posible y asegurar su supervivencia en un entorno comercial desafiante. Por lo tanto, el CGC debe considerar cómo la interrupción operativa y económica está afectando los riesgos relacionados con los incumplimiento, especialmente los delitos financieros perpetrados por personas internas y criminales fuera de la organización.

En este sentido, la industria debe poder proporcionar evidencia de que ha seguido un enfoque inteligente basado en el riesgo para cualquier medida de adaptación que haya tomado.

Si no podemos contestar a esta cuestión, tenemos un problema: ¿Tiene la organización suficiente conocimiento sobre la gobernanza y los controles dentro de los proveedores contratados y su capacidad para administrar su liquidez y el riesgo de su propio proveedor?

Cadena de suministro.

La interrupción de la cadena de suministro y solvencia de los proveedores es un problema cada vez más estructural en la industria. Ante los nuevos entornos tecnológicos, se hace cada vez más importante e imprescindible el cambio de percepción de la importancia de los riesgos relacionados con los proveedores y sus impactos en el negocio. Por ello, hay que partir de las siguientes cuestiones más apremiantes a valorar en este aspecto:

Efecto: Vinculación del proveedor /Impacto: dependencia de terceros /Situación actual: Muy presente /Cambio de valoración por importancia: Más importante

Efecto: Escalabilidad / Impacto: Aumento del riesgo / Situación actual: Muy presente / Cambio de valoración por importancia: Más importante

Efecto: Dependencia excesiva de niveles de control desconocidos / Impacto: Pérdida de control/ Situación actual: Muy presente /Cambio de valoración por importancia: Sin cambios reales; Importante

Efecto: Pérdida de Activos intangibles (información, conocimientos técnicos, etc) /Impacto: Pérdida de competitividad o extinción /Situación actual: Muy presente / Cambio de valoración por importancia: Sin cambios reales; Importante

Efecto: Escasa seguridad y trazabilidad de los controles (incluido el derecho a auditar) / Impacto: No Accountability y no Compliance / Situación actual: Muy presente / Cambio de valoración por importancia: Sin cambios reales; importante

Ejecución

En esta fase se ejecutan todos los trabajos de preparación de la instalación. Las actividades de esta fase terminan con el proceso de puesta en marcha, tras el cual se transfiere la responsabilidad de la instalación a la propiedad (el cliente). Por otra parte, el proyecto de digitalización industrial, en esta fase, también se centrará en:

- Protección de AI, atendiendo a los riesgos identificados en la fase anterior y al coste de los medios de protección, para optimizar su explotación y seguridad.
- Actividades de ciberseguridad
- Definición de responsabilidades y requisitos de ciberseguridad de todos los actores intervinientes en base a los riesgos análisis de riesgos realizado en la fase primera.
- Evaluación de seguridad

- Verificación y pruebas para verificar la correcta gestión de ciber-riesgos y de industriales y cumplimiento.
- Puesta en marcha
- No introduce novedades el modelo.
- Entrega.
- Una vez que la instalación se ha puesto en marcha en las dependencias del cliente, comienzan las pruebas de operación y las de rendimiento, que formarán parte de las pruebas de aceptación en las instalaciones definitivas

Operación y mantenimiento

Esta capa materializa un período de optimización y seguimiento inicial de la operación tras la puesta en marcha se producen frecuentes cambios para mejorar la operatividad del sistema de digitalización industrial; corregir errores de programación o de configuración que no fueron detectados durante las actividades de validación y puesta en marcha; optimizar las secuencias y lógicas de control, etc. Por otra parte, el proyecto de digitalización industrial, en esta fase, también se centrará en:

- Control y Gestión de AI
- Verificación de la efectividad y oportunidad de las medidas de protección definidas en la fase anterior.
- Verificación de la efectividad y optimización de la explotación de los Activos intangibles.
- Monitorización de incidentes
- No introduce novedades el modelo.
- Gestión cambios por incidentes
- No introduce novedades el modelo.
- Definición Planes de contingencia
  No introduce novedades el modelo.
- Control y gestión de software
  No introduce novedades el modelo.
- Control y gestión de hardware
  No introduce novedades el modelo.

- Control y gestión de accesos
  Necesidad de adaptación a la normativa de protección de datos y seguridad de la información.

- Control y gestión de redes
  No introduce novedades el modelo.

- Protección de consolas
  No introduce novedades el modelo.

- Copias de seguridad y de recuperación
  No introduce novedades el modelo.

- Formación y concienciación
  No introduce novedades el modelo.

Gobernanza y Cumplimiento

Gobernanza

Una estrategia de gobernanza integral, simplifica la administración de derechos, y ayuda a crear un modelo de gobernanza en toda la organización, que se materializa a través de la Accountability y sus revisiones periódicas.

Revisar la Gobernanza en torno a los datos del cumplimiento, verificar la confiabilidad de los informes de terceros y evaluar de forma independiente las metodologías y las entradas de datos utilizadas tanto en las operaciones como en la elaboración de estrategias a nivel ejecutivo para detectar cualquier brecha y posible error.

El CGC puede evaluar los procesos ejecutivos de toma de decisiones en busca de evidencia de que estos temas están recibiendo suficiente atención, para dar su opinión sobre si este riesgo se está gestionando en el nivel estratégico más fundamental.

Control, Auditoría y Cumplimiento

Con la creciente necesidad de auditoría y cumplimiento, los informes de auditoría se vuelven críticos. Esta capa define la estrategia de informes para la ciberseguridad, protección de activos intangibles y cumplimiento en cuanto a las tecnologías de digitalización industrial para cada proyecto de digitalización industrial.

Se debe controlar y revisar que se está aplicando la visión de 360 grados de la tercera línea del negocio para ayudarlo a mitigar sus riesgos de cumplimiento cibernético.

Se debe controlar y revisar si la función de cumplimiento está al tanto de todas las leyes y regulaciones de aplicación existentes y futuras que se aplican al negocio en las diversas jurisdicciones en las que está presente.

Se debe controlar y revisar si se han traducido las metas y los objetivos en cumplimiento y controles de Gobernanza y Cumplimiento, incluidos los KPI que indican el progreso en relación con los objetivos.

Se debe controlar y revisar cómo mide e informa la empresa su progreso en el logro de sus objetivos de Gobernanza y Cumplimiento.

El CGC debería revisar la confiabilidad de estos informes de terceros o de auditoría interna.

CONCLUSIÓN

El creciente número de incidentes relacionados con la violación de seguridad, y los costes asociados, han puesto un mayor énfasis en la necesidad de una implementación de seguridad avanzada, entendida de una manera holística. A medida que aumente la digitalización industrial, con el uso de la infraestructura de nube, Internet de las cosas, las experiencias de movilidad y otras innovaciones digitales emergentes, las organizaciones industriales tendrán que mirar más allá de los medios de seguridad tradicionales y optar por una implementación integral de Gestión de Activos Intangibles junto a la Gobernanza y el Cumplimiento. El marco expuesto en este documento puede actuar como punto de partida en su camino hacia un panorama de Ciberseguridad Industrial evolucionado, alineado con el cumplimiento desde el Buen Gobierno, resiliente y a prueba de futuro.

UNA PROPUESTA DE CUMPLIMIENTO Y ACCOUNTABILITY EN BASE A EVIDENCIAS DIGITALES PARA EL COMPLIANCE TECNOLÓGICO

Seguimos analizando la ciberseguridad como requisito del Compliance en la industria. Por este motivo, centrándonos en la parte digital y tecnológica del Compliance y basándome en el documento "Análisis forense en SCI 2016" del CCI planteamos esta propuesta de Cumplimiento.

Para ello, recordemos que el cumplimiento corporativo o Compliance tiene el objetivo de dotar a las empresas de un sistema eficaz de Gestión de Compliance (Cumplimiento normativo) con el objetivo de evitar los riesgos de incumplimiento legal, es decir, minimizar los riesgos de sufrir sanciones, multas, contingencias, daños reputacionales etc. (ISO 19600)

Resulta de vital importancia documentar todo el proceso, la UNE 19601 además establece que es de vital importancia para la organización tener la información documentada, es decir que deben estar documentados todos los acuerdos, procesos, políticas, verificaciones, comunicaciones del modelo, etc. a fin de poder acreditar su existencia, su integración en la organización y su uso en los procesos habituales de la persona jurídica y en la toma de decisiones de los órganos correspondientes.

Por este motivo, la ausencia de plan de cumplimiento antes de la comisión del delito impide la aplicación de la exención de responsabilidad para las personas jurídicas, que contempla el art. 31 bis 2 y 4 CP; además esa exención de responsabilidad no siempre será total, esto es, se gradúa la responsabilidad, ya que el propio texto habla de "medidas idóneas" o "modelo adecuado" y como por otro lado se aplica para las personas físicas en el art. 21. 1.ª CP cuando no concurren todos los requisitos de exención. De lo que se concluye que resulta imprescindible que se pueda probar, o que existan evidencias de que se encuentra implantado un sistema de Compliance. En el ámbito industrial, es igualmente necesario que sea posible probar mediante evidencias la existencia de un sistema de Compliance.

Al igual que para ganar un pleito, tan importante es tener razón, como saber probar que se tiene derecho a aquello que se solicita, en el Compliance es imprescindible implantar el Sistema de Compliance y tener la capacidad de probarlo. Lo que pone de manifiesto la relevancia práctica, por un lado, de gestionar de una manera adecuada la documentación y archivos del Sistema, y por otro lado, de la actividad probatoria y la necesidad de conocer debidamente los aspectos más destacados de la misma. En este artículo, analizaremos la actividad probatoria proactiva, o generación de evidencias tecnológicas o digitales, del Sistema de Compliance Industrial, a través del análisis forense informático. Utilizamos el análisis forense informático como herramienta para generar pruebas de Cumplimiento desde el diseño.

El análisis forense informático es un conjunto de técnicas y metodologías generalmente aceptadas que tienen por objeto la obtención de evidencias con valor probatorio. Las evidencias pueden acabar, como medio de prueba, en un proceso judicial, ser usadas internamente en las organizaciones para alimentar su cuadro de mandos y ofrecer una imagen fiel de la operación de los sistemas (proporcionando información de valor para la conformidad, el control interno o la auditoría), o pueden ser usadas en la investigación de un incidente dentro de una compañía. En nuestro modelo, pretende integrar la generación de evidencias como pruebas y proporcionar información para la conformidad, el control interno y la auditoría.

Por este motivo, es necesario partir de la definición de evidencia electrónica, que es un registro de la información y datos guardada, transmitida o difundida por un dispositivo electrónico que puede utilizarse como prueba en un proceso judicial, o para probar la existencia de un sistema de Compliance eficaz realmente implantado. Es cualquier dato digital que pueda relacionar un delito o incumplimiento con su víctima o con su autor.

Para ello, es imprescindible partir del estado en que se puede encontrar la información en la industria y sus características.

En este sentido, encontramos la información almacenada estáticamente, que es la que se encuentra almacenada en un repositorio de información en espera de ser recuperada o utilizada. Esta información puede ser susceptible de pérdida por borrado automático, por procesos de comandos activados automáticamente en acciones de arranque o paro del dispositivo.

También, podemos distinguir la información almacenada dinámicamente o en procesamiento, encontrándose almacenada temporalmente en un elemento volátil en espera de ser utilizada, o en proceso de utilización, por lo que puede perderse a causa de acciones precipitadas o por apagado del dispositivo, o susceptible de borrado automático por procesos de comandos en acciones de paro del dispositivo.

Por último, podemos distinguir la información en tránsito, que se encuentra en movimiento por la red en forma de paquete de información que puede ser capturado y/o almacenado en medios adecuados.

Los dispositivos digitales están en todas partes en el mundo de hoy, ayudando a las personas y máquinas a comunicarse local y globalmente con facilidad. Estos dispositivos son mucho más que los ordenadores, los teléfonos móviles e Internet, porque cualquier pieza de tecnología que procese información puede usarse de manera criminal o puede generar evidencias útiles para Compliance.

Por ejemplo, los dispositivos IoT pueden llevar mensajes codificados entre delincuentes e incluso podrían usarse para almacenar, ver, compartir o manipular imágenes ilegales o información. Lo importante es saber que debemos ser capaces de reconocer y generar y aprovechar adecuadamente la evidencia digital potencial para Compliance.

Dependerá de la tipología de los dispositivos en los que queramos generar evidencias, la concreción de los diferentes procesos de recopilación de evidencia, herramientas y preocupaciones de la industria en cuestión.

En este sentido, es evidente que en infraestructuras industriales críticas, como en otros entornos, el restablecimiento de las operaciones es la máxima prioridad, pero también, dentro de un ciclo de mejora continua, resulta fundamental conocer lo ocurrido, aprender de los errores, establecer medidas de mitigación para evitar incidentes en el futuro y generar evidencias que prueben cómo se ha materializado lo ocurrido desde la óptica del Compliance. A tal fin, extraer, preservar y analizar las evidencias electrónicas permitirá generar pruebas para realizar un posterior análisis forense que ayude a comprender lo ocurrido e identificar a los responsables.

El primero de los grupos presupone un desafío en entornos industriales, especialmente cuando no es posible detener los equipos o procesos en funcionamiento. Por esta razón, en muchas situaciones será necesario recolectar evidencia en vivo, es decir, mientras el sistema se encuentra operando, aun en condiciones provocadas por el incidente que intentamos analizar. Por ello, proponemos hacerlo de manera proactiva desde el diseño o, en su defecto, desde la configuración e integrando métodos de generación y recolección de evidencias automatizado desde la óptica del Compliance.

En cualquiera de estas situaciones, se deja un rastro electrónico de información que un equipo de investigación puede reconocer, aprovechar y explotar. En el caso que estamos exponiendo, y atendiendo a las limitaciones existentes en los entornos de operación de la industria, lo que debe establecerse, si es posible desde el diseño, es la generación de estos rastros electrónicos de información y datos que sirvan para, en su caso, reconocer, aprovechar y explotar dichas evidencias como prueba de la implantación del sistema de Compliance, de sus medidas de cumplimiento y de seguimiento y control. La generación de evidencias debe seguir los procedimientos adecuados para generar datos más valiosos. No seguir los procedimientos adecuados para dicha generación puede conllevar una pérdida de la evidencia o una evidencia dañada o inadmisible en el tribunal y que irá en detrimento del Compliance.

Los requisitos que debe cumplir una evidencia digital para ser admitida como prueba en un juicio son:

• Auténtica: debe haber sido generada - obtenida y registrada en el lugar de los hechos y debe garantizarse la integridad de los archivos.

• Confiable: esta evidencia digital debe proceder de fuentes fiables. Es decir, es confiable si el sistema que la produjo no ha sido violado y funcionaba correctamente cuando se generó o guardó esa prueba.

• Integra: para que esa prueba sea suficiente debe estar completa.

• Cumplir las reglas del poder judicial: es necesario que esa evidencia sea acorde con las leyes y disposiciones vigentes en el ordenamiento jurídico. Sobre todo a la hora de recabar información y datos de manera global para garantizar la seguridad e integridad de la información y de la operación sin vulnerar derechos de terceros.

Estos requisitos deberían cumplirse en la generación y recolección de evidencias digitales desde el diseño o, en su defecto, desde la configuración, con el objeto de generar prueba de Compliance.

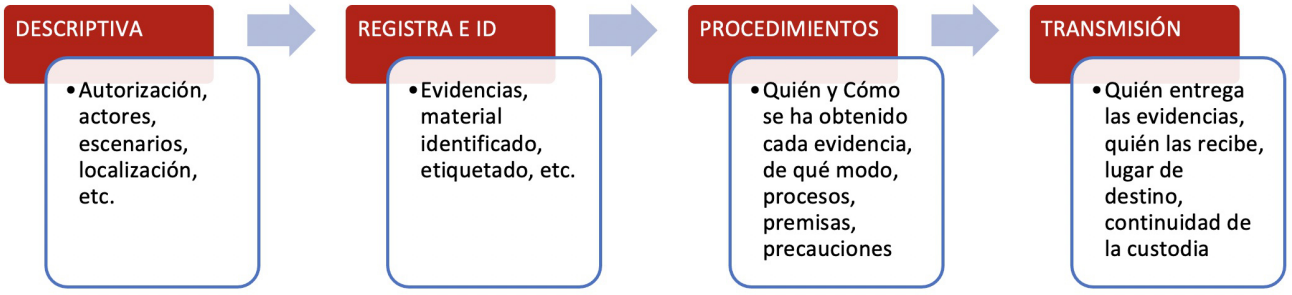
Las evidencias digitales deben custodiarse, protegerse, controlarse y etiquetarse y para ello habrá que determinar la manera y responsables de dicha custodia.

Para garantizar la generación, custodia y el análisis más preciso de la evidencia, se tendrán que implementar políticas y procedimientos que rigen instalaciones y equipos, métodos y procedimientos desde el diseño o, en su defecto, desde la configuración.

La actuación de campo para la generación y recopilación de pruebas y evidencias informáticas en dispositivos electrónicos que contienen información o datos ha de realizarse atendiendo la buenas prácticas contenidas en la RFC-3227 “Guidelines formevidence Collection and Archiving” (2002); la ISO/IEC 27037 “Guidelines for identification, collection, acquisition and preservation of digital evidence (2009); en la UNE 71505 “Sistema de gestión de Evidencias Electrónicas” y la UNE 71506 “Metodología para el análisis forense de las evidencias electrónicas” (2013). El objetivo es garantizar la originalidad, la identificación, el registro, la no contaminación y la preservación de las evidencias recopiladas. Igualmente, es imprescindible atender a la ISO 15489 de “Sistema de Gestión de Documentos y Archivos”.

Para que la actuación de campo sea un proceso completo se han de cubrir las funciones: Descriptiva, Registral e Identificativa, de Procedimiento y de Transmisión de la custodia. Eso se recoge en un documento denominado “Protocolo de actuación”. Protocolo de actuación desde el diseño o, en su defecto, desde la configuración en nuestra propuesta.

En la ejecución de la actuación de campo para la generación y recopilación de pruebas y evidencias digitales, además de la generación y recopilación de las mismas, se ha de realizar una descripción del escenario o el entorno para contribuir a crear una idea clara del contexto en el que se genera la prueba o evidencia digital. Si existen situaciones complejas, se pueden utilizar grabaciones de video en el que se visualice el proceso. Ello nos permitirá describir el proceso de generación, recopilación y preservación.



En la ejecución de la actuación de campo para la generación y recopilación de pruebas y evidencias digitales, además de la generación y recopilación de las mismas, se ha de realizar una descripción del escenario o el entorno para contribuir a crear una idea clara del contexto en el que se genera la prueba o evidencia digital. Si existen situaciones complejas, se pueden utilizar grabaciones de video en el que se visualice el proceso. Ello nos permitirá describir el proceso de generación, recopilación y preservación.

También es necesario hacer una descripción de la prueba o evidencia, su tipología, características, cómo y dónde se ha generado, en qué condiciones o circunstancias, etc.

Normalmente, en cada tipología de evidencia y especialidad existen unos protocolos y estándares de buenas prácticas para garantizar que el proceso seguido en la obtención (en nuestro caso generación) es el adecuado para la evidencia o prueba recopilada o generada, mostrándose que se ha ejecutado de forma correcta y se preserva la evidencia en las condiciones y medios adecuados.

En todo caso, resulta imprescindible determinar las siguientes cuestiones al respecto:

- Qué evidencias o pruebas son necesarias generar y recopilar.
- De qué modo se van a generar y recopilar.
- Qué precauciones y comprobaciones deben realizarse sobre su generación y recopilación.
- Cómo se han de preservar.
- Cómo se han de manipular para no perder la integridad.
- Descripción de la cadena de custodia, en su caso.

Igualmente, será recomendable la gestión de un registro o inventario de pruebas o evidencias. Toda evidencia se deberá identificar unívocamente mediante un código de identificación.

Las recomendaciones de la RFC 3227 (Request for Comments 3227) sobre "Recopilación y archivo de evidencias" establecen unas actuaciones básicas para la captura de evidencias, entre las cuales destacan las de generar checksums (de tipo HASH, por ejemplo) y firmar criptográficamente las pruebas con la finalidad de preservar la cadena de custodia siempre que estas actuaciones no alteren la prueba.

Centrémonos ahora en algunas de las peculiaridades de las Tecnologías de la Operación en el ámbito industrial. Para ello, diferenciaremos los Sistemas de Control Industrial, las Redes Industriales y la Integración con los sistemas corporativos.

En Sistemas de Control Industrial

Nos centramos en los principales componentes de los ICS (Sistemas de Control Industrial) y que podemos dividir en sistemas de control y sistemas de supervisión.

Respecto a los sistemas de control, encontramos los sistemas de control individual de cada recurso. Entre ellos, podemos identificar PLCs (Controladores lógicos programables) y RTUs (Unidades de terminal remotas) de gama baja y media, sistemas de control numérico, transporte automatizado, etc.

Dichos sistemas utilizarán los datos del proceso proporcionados por los equipos del nivel instrumentación y se darán las consignas a los actuadores y máquinas de dicho nivel.

También dentro de este nivel, involucrados directamente en el proceso de control, podemos encontrar algunos equipos que se ejecutan sobre un sistema operativo común, tales como Windows, Unix o Linux. Un ejemplo de este tipo de equipos son los que soportan comunicaciones OPC, u otro tipo de gateways de comunicaciones.

En cuanto a los sistemas de supervisión, se encuentran sistemas que controlan la secuencia de fabricación y/o producción (y que pueden dar las consignas al nivel de campo).

En este nivel se emplean PLCs de gama media y alta, PCs Industriales, HMI, SCADA, DCS y equipos, como ordenadores portátiles, ordenadores de sobremesa, estaciones de trabajo y servidores que ejecutan sus aplicaciones en un sistema operativo común, como Windows, Unix o Linux. Estos equipos a menudo son empleados para proporcionar histórico de datos, programación y/o funciones de supervisión…etc.

Lo más frecuente es encontrarse que el análisis forense para ICS se concentra en el nivel de supervisión, sistema SCADA, DCS, bases de datos…etc. La principal razón es que normalmente estos sistemas funcionan sobre sistemas operativos de propósito general, como Windows, Unix o Linux, y por tanto responden a incidentes que podemos investigar con las herramientas forenses disponibles para estas plataformas, y a su vez, los ataques más comunes en los ICS ocurren a este nivel (ataques de malware, de explotación de vulnerabilidades sobre los HMI o el software de los SCADA o DCS, etc.). Sin embargo, es importante también analizar los sistemas del nivel de control, aunque en este caso, las herramientas disponibles para estas plataformas sean escasas.

En ambos niveles nos deberemos centrar en las diferentes categorías de análisis existentes (fallos o ataques a través de configuración de sistemas de control, fallos o ataques de la configuración del sistema operativo o de aplicaciones de sistemas de supervisión, fallos o ataques a través de redes Ethernet u otras comunicaciones, fallos o ataques a través de dispositivos de almacenamiento o aplicaciones de intercambio) para concretar el modo de actuar para generar y recopilar las evidencias electrónicas que pretendemos para Compliance desde el diseño o, en su defecto, desde la configuración.

En este ámbito, el objetivo será generar y recopilar evidencias electrónicas desde el diseño o, en su defecto, desde la configuración de cómo se produjo el compromiso, bajo qué circunstancias, la identidad del posible atacante o incumplidor, su procedencia y origen, los objetivos del atacante, los efectos del compromiso y la secuencia temporal de los eventos.

La vulnerabilidad principal a nivel de control que deberíamos observar desde el Compliance sería la no incorporación de requisitos de ciberseguridad desde el diseño o, en su defecto, desde la configuración, lo que puede provocar ataques que ejecuten código arbitrario, obtengan privilegios, accedan a ficheros con información de entrada al controlador, capturen tráfico de entrada/salida y provoquen situaciones de denegación de servicio, escalado de privilegios, control remoto del sistema, alteración o acceso a la memoria, entre otros.

Las vulnerabilidades principales a nivel de supervisión que debemos tener presentes desde el Compliance son la autenticación débil o nula, acceso a credenciales en comunicaciones no cifradas, inyección de código arbitrario, obtención y escalado de privilegios, segregación de roles y perfiles ineficientes, configuraciones por defecto, control remoto del sistema, etc.

Los pasos a seguir para la generación de evidencias electrónicas en este ámbito serían: Enfocar desde el entorno (Entorno de operación, servicios y procesos automatizados, arquitectura y documentación); Identificar a sospechosos; Determinar el alcance respecto a los sistemas implicados, atendiendo a los sistemas, la red y los dispositivos conectados; los sistemas operativos implicados en el PLC y el diseño e implementación de redes; y la volatilidad de la información. El objetivo será diseñar un modelo de obtención de evidencias en el entorno, desde el diseño o, en su defecto, desde la configuración, atendiendo a la ubicación física de los dispositivos de control, las especificaciones de hardware y software de los ICS, especificaciones del hardware y software de dispositivos de red, mapa de red, especificaciones de parametrización y lógica de control, especificaciones de hardware y software de sistemas del nivel, flujogramas del proceso y características de uso de componentes, las conexiones desde y hacia ubicaciones asociadas o por pares, el acceso utilizado por el proveedor de soporte, la eficacia de las políticas de seguridad que regulan las operaciones de control, etc. La evidencia digital resultante deberá ser preservada para asegurar su integridad junto a toda la documentación sistemática relacionada. Para ello, podemos apoyarnos en herramientas y técnicas de forensic, tanto a nivel de hardware, de software.

En Redes Industriales

En este sentido, tal y como dijimos con anterioridad, el análisis de los datos de una red es diferente del análisis de datos encontrados en un disco duro debido a la naturaleza temporal de la información en la red (información en tránsito).

Un análisis forense de una red de operación industrial (MES) implica, por tanto, la monitorización del tráfico de red para determinar si existe una anomalía en el tráfico y comprobar si ésta supone alguna actividad no autorizada que podría alterar o poner en riesgo a los ICS.

Para determinar los sistemas de análisis forense en redes, deberemos atender al tipo de sistemas que vamos a utilizar, sistemas “catch ir as you can” en el que todo el tráfico para por un punto y es registrado en el sistema de almacenamiento de la información, o sistemas “stop, look ad listen” análisis en memoria, y a los requerimientos, garantías legales o autorizaciones exigibles en cada caso en relación a la intimidad.

Siguiendo la norma NIST SP800-86 “Guía para integrar técnicas forenses de respuesta a incidentes”, los pasos a seguir para la generación y recopilación de evidencias electrónicas en este ámbito, deben ser definir e implementar desde el diseño o, en su defecto, desde la configuración, la manera de capturar las

evidencias, esto es identificar, marcar, grabar y adquirir datos de las posibles fuentes relevantes, siguiendo las directrices y procedimientos que preservan la integridad de los datos. Para ello, podemos apoyarnos en herramientas y técnicas de forensic a nivel de red.

En la integración con los sistemas corporativos

Por análisis forense en la integración con los sistemas corporativos, se entiende el proceso de búsqueda detallada para reconstruir a través de todos los medios posibles, el registro de acontecimientos que tuvieron lugar desde el momento en el que los sistemas que permiten la integración entre los ambientes OT e IT estuvieron en su estado integro, hasta el momento de detección de una intrusión o ataque. Esto resulta de mucha utilidad desde la perspectiva del Compliance con carácter previo a que suceda el acontecimiento y generar registros de acontecimientos automatizados desde el diseño o desde la configuración.

El análisis forense de este apartado conlleva la recogida de datos, examen y análisis de ficheros, datos de sistemas operativos y datos del tráfico de red entre la zona corporativa (IT) y la zona de operación y control (OT), incluyendo los dispositivos y los datos de las aplicaciones ubicadas en la zona desmilitarizada (DMZ, por sus siglas en inglés). Involucra a los sistemas de red de operación (MES) y a la de red de información (ERP).

La red DMZ permite segregar los sistemas de red de operación y la red de información. Los sistemas y aplicaciones en el sistema de red de operaciones se comunican con los sistemas de red de información. La comunicación directa entre los sistemas en la zona fabricación y zonas de empresas no se recomienda. Entre los sistemas de red de operación y a la de red de información se suele disponer de un cortafuegos y entre los sistemas de red de operación y los sistemas de supervisión también se tiene otro cortafuegos.

La vulnerabilidad de la DMZ se asocia a la mala configuración de los cortafuegos debido a políticas de seguridad no diseñadas correctamente o viciadas por razones históricas. Para ello, desde el punto de vista de Compliance, será imprescindible la instalación de sistemas de detección de intrusos en los segmentos de redes del DMZ y la correcta configuración de los cortafuegos.

Los sistemas de detección de intrusos deben ser desplegados convenientemente en toda la red y configurados para detectar los ataques que tienen más probabilidades de tener éxito. Las técnicas y procesos para recoger, examinar y analizar datos ya expuestas son igualmente válidas para la integración con sistemas corporativos por lo que solo se incluirá los pasos básicos de análisis que pueden ser particulares de las aplicaciones que se ubican en la DMZ, de los dispositivos utilizados para interconectar la zona de confianza con la zona potencialmente hostil, y de las transacciones y tráfico de datos entre las distintas zonas.

Los mensajes de registro deben contener atributos del sistema pertinente, como direcciones IP, puertos y protocolos utilizados, día y hora, nombre de usuario, el método de acceso tales como FTP, SSH o HTTP desde el diseño o, en su defecto, desde la configuración. Al correlacionar los registros de eventos de diferentes sistemas, los sellos de tiempo en que ocurren se convierten en un factor importante. Por ello es recomendable que los sistemas y aplicaciones que generan registros de eventos utilicen la misma hora fuente, un protocolo corporativo de hora de red, permitiendo registros con sellos de tiempo precisos.

Los eventos mínimos que se deben registrar, recopilar y custodiar son: acceso a cortafuegos, accesos remotos, eventos detectados por el sistema de intrusión, acceso y eventos en los servidores, eventos en las aplicaciones. Todo ello desde el diseño o, en su defecto, desde la configuración.

El servidor de recopilación de registros debe estar correctamente dimensionado, con espacio suficiente para almacenar los registros de sucesos para un período de retención de datos apropiado para cada caso. El período de retención debe documentarse en la política de ciberseguridad y debe tener en cuenta las regulaciones que afecten al sector industrial al que pertenece la organización.

APLICACIÓN DEL RD 43/2021, REGLAMENTO DE DESARROLLO DE LA TRANSPOSICIÓN DE LA DIRECTIVA NIS

Desde marzo de 2021 me han consultado en diversas ocasiones y diferentes industrias, sobre todo del sector de tratamiento y distribución de aguas, varias cuestiones sobre la aplicación del RD 43/2021, reglamento de desarrollo de la transposición de la Directiva NIS. Por este motivo, el interés de este artículo para aclarar este aspecto.

La cuestión principal, se plantea sobre su aplicación. La duda surge de la redacción del propio Real Decreto. El artículo 2.1.a) dice que se aplicará a los prestadores de servicios esenciales (...) comprendidos en los sectores estratégicos de la Ley 8/2011 (Ley PIC). Por su parte, el párrafo del artículo 2.2.a) señala que "la identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011". La cuestión muy repetida es ¿Significa esto que SOLO los operadores que hayan sido identificados según los procedimientos de la Ley PIC quedan bajo el ámbito de aplicación de este RD?

Pasemos a abordar esta cuestión, teniendo en cuenta que:

El artículo 1 RD 43/2021 señala "Este real decreto tiene por objeto desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad."

Por lo tanto, artículo 2 del RD 43/2021 desarrolla el Real Decreto-ley 12/2018 (de hecho tiene un alcance muy alineado y común):

- el marco estratégico e institucional de seguridad de redes y sistemas de información.
- la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.
- la gestión de incidentes de seguridad.

Por su parte, el Real Decreto-ley 12/2018 define:

c) **Servicio esencial:** servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

d) **Operador de servicios esenciales:** entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.

e) **Servicio digital:** servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

f) **Proveedor de servicios digitales:** persona jurídica que presta un servicio digital.

Atendiendo a lo expuesto respecto al operador de servicios esenciales, el artículo 6 Real Decreto-ley 12/2018 establece respecto a la identificación de servicios esenciales y de operadores de servicios esenciales:

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.
La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

Por tanto, a la pregunta que se platea, hay que responder que:

Respecto a los servicios esenciales y los operadores que los presten, la respuesta es SI, si una compañía NO HA SIDO clasificada como operador esencial, no le aplica -por ahora- el RD.

Respecto a los servicios digitales y proveedores de servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube y que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. NO es necesario tal clasificación para su aplicación.

PASEO DE LAS DELICIAS, 30 - 2°
28045 MADRID

+34 910 910 751

INFO@CCI-ES.ORG
WWW.CCI-ES.ORG
BLOG.CCI-ES.ORG
@INFO_CCI